

NORTHERN DISTRICT OF TEXAS
FILED

UNITED STATES DISTRICT COURT

for the
Northern District of Texas

DEC - 9 2019

CLERK U.S. DISTRICT COURT

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

5409 Windy Meadow Drive
Arlington, Texas 76107

By: _____

Case No.

4:19-mj-946

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

5409 Windy Meadow Drive, Arlington, Texas 76107, as further described in Attachment A.

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252 and 2252A	Distribution, Transportation, Receipt and Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of HSI Special Agent Elmore Armstrong, Jr.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

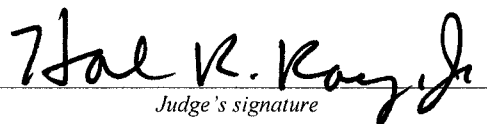
Special Agent Elmore Armstrong, Jr., HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

12/9/2019



Judge's signature

City and state: Fort Worth, Texas

Hal R. Ray, Jr., U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT
APPLICATION

I, Elmore Armstrong, Jr., being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since June 2008. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an “investigative or law enforcement officer of the United States” within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to the sexual exploitation of children, including the illegal production, distribution, transportation, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received extensive training in the area of child exploitation, and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in numerous child pornography investigations, and I am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is being made in support of an application for a warrant authorizing the search of the residential property at **5409 Windy Meadow Drive, Arlington, Tarrant County, Texas, 76017**, located within the Northern District of Texas, and further described in Attachment A incorporated with this affidavit. I seek the authorization to search the entire residential premises, including any attached or unattached outbuildings, and any computers and computer media located therein, for the items specified in Attachment B incorporated with this affidavit, which constitute contraband, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, which make the transportation, distribution or possession of child pornography a federal offense.

4. The information set forth in this affidavit comes from my investigation, my training and experience, and information provided to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are presently located within **5409 Windy Meadow Drive, Arlington, Texas**.

DEFINITIONS

5. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and Attachment B:

a. “Computer” refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, “computer” also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. See 18 U.S.C. § 1030(e)(1).

b. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider assigns a different unique number to a

computer every time it accesses the Internet. IP addresses may also be static, which means the provider assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

d. "Mobile applications" or "mobile apps" are computer programs or software applications specifically designed to run on mobile devices (e.g., smartphones, tablets, e-readers, etc.). Mobile applications are generally downloaded from application distribution platforms operated by specific mobile operating systems, like App Store (Apple mobile devices) or Google Play Store (Android mobile devices).

e. "Instant messaging" is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating and gaming websites and mobile applications offer instant messaging for users to communicate amongst themselves. More advanced features of instant messaging include push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

f. A "hash value" is value given to a file or data after a mathematical function converts the data into an alpha-numeric value. A hash value is akin to a digital fingerprint, in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. A hash value is unique to the specific data from which the hash value was generated.

Hash values can be used to search for identical data stored on various digital devices, as identical data will have the same hash value.

g. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks or DVD’s, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Based on my training and experience in child exploitation investigations, I am aware that computers, computer technology, and the Internet significantly facilitate the receipt, distribution, and possession of child pornography. Computers generally serve five (5) functions in connection with child exploitation offenses: production, communication, distribution, storage and social networking.

Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Therefore, through use of the Internet, electronic contact can be made to literally millions of computers around the world.

7. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as smartphones (e.g., Apple iPhones, Samsung Galaxy), connected devices (e.g., Apple iTouch), e-readers, and tablets (e.g., Apple iPads, Kindle Fire) now function essentially as computers with the same abilities to store images in digital form.

8. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including, but not limited to, services offered by Internet portals such as Yahoo, Outlook, and Google. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats.

A user can set up an online storage account from any computer or device with access to the Internet, and evidence of such online storage of child pornography is often found on the user's computer or device.

9. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive in space that is not allocated to an active file for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

10. Additionally, files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically maintain a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

SPECIFICS REGARDING THE SEARCH AND SEIZURE OF COMPUTERS

11. Based on my training and experience, I am aware that the search of computers often requires agents to seize most of the computer items (e.g., hardware, software, and instructions) to be processed later by a qualified computer expert in a

laboratory or other controlled environment. That is essential to the search for electronic evidence because of the following facts:

a. Computer storage devices, like hard drives, diskettes, tapes, or laser disks, store the equivalent of thousands of pages of information. When the user wants to conceal electronic evidence of a crime, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included within the scope of warrant. This process can take weeks or months, depending on the volume of the stored data, and it would be impractical to attempt this kind of data search on-site;

b. Searching computer systems for criminal evidence is a highly technical process that requires expert skills and a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in specific systems and applications. It is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system can be equated to a scientific procedure, which is designed to protect the integrity of the evidence while recovering hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction, both from external sources and from code embedded in the system as a "booby-trap," the controlled environment of a laboratory is essential to its complete and accurate analysis;

c. In order to fully retrieve data from a computer system, an analyst needs all magnetic storage devices, as well as the central processing unit (CPU). For child pornography investigations, in which the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. The analyst needs all assisting software (e.g., operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data, as well as all related instructional manuals, documentation and security devices;

d. Searching computerized information for evidence or instrumentalities of a crime often requires the seizure of the entire computer's input/output periphery devices, including related documentation, passwords and security devices, so that a qualified examiner can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system; therefore, it is important that the analyst be able to properly retrieve the evidence sought.

12. The facts set forth in this affidavit establish probable cause to believe that a computer, its storage devices, and other system components were used as a means of committing offenses involving the sexual exploitation of minors, in addition to storing evidence of said crime.

Accordingly, I seek the authorization to seize and search any computers and related electronic devices located at **5409 Windy Meadow Drive, Arlington, Texas**, consistent with Attachment B to the requested warrant.

USE OF HASH VALUES TO UNIQUELY IDENTIFY FILES

13. A hash is a mathematical function which converts file data into an alphanumeric value. A hash value is a string of characters obtained by processing a file's contents through an algorithmic function. There are various types of hash functions, including, but not limited to the Secure Hash Algorithm (SHA) and Message-Digest Algorithm 5 (MD5). A hash value is unique to one specific file. A file can be copied and renamed; but if it is an exact copy, regardless of the name of the file, it will have the same hash value. An example of a hash value would be "86F7E437FAA5A7FCE15DIDDCB9EAEAEA377667B8."

14. Hash values are regularly used to compare the contents of one file against another. By comparing the hash values, one can conclude whether the files are identical with a 99.999 percent certainty. A hash value is often described as the "fingerprint" of a digital file. Based on my experience in child exploitation investigations and information provided by other law enforcement sources, I am unaware of any documented occurrences in which two different files on the Internet, which contained different contents, were found sharing the same hash value.

15. As a result of the uniqueness and reliability of hash functions, hash values have become an instrumental tool for private companies and law enforcement to combat the online distribution of child pornography. Hash values allow private companies and law enforcement organizations to rapidly compare the hash values of suspect files against the hash values of known child pornography files that are in circulation, all without the need for a human investigator to sort through the material. In the United States, many Electronic Service Providers (ESPs) compare user-uploaded files against the hash values of known child pornography files, and report any “hash matches” to the National Center for Missing and Exploited Children (NCMEC).

INFORMATION ABOUT MICROSOFT PHOTO DNA

16. PhotoDNA is a technology developed by the Microsoft Corporation that computes a unique hash value for image files. The primary difference between the PhotoDNA hash function and other hash functions is that PhotoDNA hashes are computed in a way that is resistant to file alterations. The PhotoDNA algorithm creates a unique hash value for a file that can be compared to the hash values of other files to find copies of the same image. Specifically, the PhotoDNA algorithm hashes an image into a black-and-white format and uniform size, then divides the image into several sections that are assigned a numerical value. Together, these values compose the PhotoDNA hash value for the image; so even when an image is altered (cropped, color-change, etc.), PhotoDNA can recognize and identify the image as a copy through the sections that were not altered.

17. Many companies in the United States and elsewhere use PhotoDNA to compare images uploaded by their users against a database of known child pornography images. This allows companies to quickly identify images and copies of images depicting child pornography without a human being having to look at the images again. Microsoft donated PhotoDNA to NCMEC, and the software is available to private companies and law enforcement organizations.

INFORMATION ABOUT KIK MESSENGER

18. Kik Messenger (hereinafter, “Kik”) is a free instant messaging mobile application designed and managed by Kik Interactive Incorporated, a company based in Waterloo, Canada.¹ Kik uses the Internet to allow users to send and receive instant messages, photos and videos, and to engage in video chat. During the account registration process, users are prompted to create a username, which cannot later be changed, and a display name, which other users initially see when communicating. During the registration process, users are also asked to provide an email address, date of birth, user location and a profile picture. Email addresses can be “confirmed,” which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or “unconfirmed,” which means the email address is invalid, or the user did not click on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process.

¹ Kik was recently purchased by MediaLab, a U.S.-based technology company headquartered in California. At all times relevant to this investigation, Kik was owned by Kik Interactive in Canada.

Affidavit in Support of Application for Search Warrant – Page 12 of 24

19. Once an account is created, a user is able to locate other users via a search feature. The search feature generally requires a user to know an intended recipient's username to locate them. Once connected, Kik users can share messages, images and videos, or engage in video chat. Kik also allows users to create chatrooms, through which groups of up to 50 users can exchange messages and digital files. These chatrooms, commonly referred to as "Kik Groups," are administered by the user who created the chatroom, and this user has the authority to add, remove, and ban other users from the group. These groups are normally created with a group code that contains a "hashtag" (e.g., "#KikTeens"), allowing the group or chatroom to be located more easily. Once a group is created, Kik users can engage in a "group chat" and exchange messages and content.

20. According to Kik's Terms of Service, which each user must acknowledge when creating an account, it is a violation of the agreement to use Kik to upload, post, comment on, or store content that is obscene, offensive, contains pornography, or is harmful to minors in any way. These Terms of Service specifically state that "...[Kik] may review, screen and delete your User Content at any time if we think it may violate these Terms. You are responsible for the User Content that you send through the Services, including for back up of such content."

21. To combat the proliferation of child pornography on its platform, the Kik Trust and Safety Team uses a third-party company to review profile pictures that are uploaded by users and groups.

Kik also uses PhotoDNA to compare user-uploaded images against a database of known child pornography images that are in circulation. Any images that are flagged and reported by the third-party company or the PhotoDNA software are subsequently viewed by a member of the Kik Trust and Safety Team.

22. Kik also allows users to report other users who have abused or harassed them within the app. These are referred to as “Abuse Reports.” When a Kik user submits an Abuse Report, they can include their full conversation history, including text and any images or videos transmitted in the conversation. When Kik receives an Abuse Report, an employee reviews the reported material to verify that it contains child pornography or is otherwise considered child exploitative material.

23. Any material determined by Kik to be exploitative through PhotoDNA hash match, third-party monitoring or Abuse Reports is subsequently reported to the Royal Canadian Mounted Police (RCMP). Kik provides the RCMP with the reported material, as well as basic subscriber information for the suspect account. This subscriber data includes, but is not limited to, the information entered by the user during the account registration process, any updates to this information after the registration process, device type (e.g., iPhone, Samsung Galaxy S5, etc.), and log-in data associated with the last thirty days of account activity. Upon reporting this information to the RCMP, Kik deletes the suspect account for violating its Terms of Service.

24. Based on my training and experience in child exploitation investigations, I am aware that Kik is a prominent meeting place for individuals seeking to share child pornography and engage in child exploitative dialogue. I have arrested several offenders who used Kik to transport, distribute, and receive child pornography, as well as other offenders who used the platform to coerce and entice minors to engage in illegal sexual activity. Based on information obtained from interviews with some of these offenders, I am aware that Kik is a preferred platform for child exploitation offenders because the application facilitates anonymous communication, which assists offenders in avoiding detection by law enforcement.

FACTS IN SUPPORT OF PROBABLE CAUSE

Kik User “bjm0907”

25. On or about May 13, 2019, Kik user “bjm0907” uploaded an image file that was flagged by PhotoDNA for having a hash value associated with a known child pornography image. A Kik employee viewed the image to confirm it contained child pornography, and per Kik’s protocol, the information was subsequently reported to the RCMP. The information provided for this account included the following subscriber information:

Username: bjm0907
First Name: Matt
Last Name: Q
Email: jwm@sbcglobal.net (unconfirmed)
Birthday: [redacted]1981
Device Type: Apple iPhone
Upload IP address: 76.184.73.204

26. RCMP personnel researched IP address 76.184.73.204 and learned that it resolved to the United States. The RCMP subsequently forwarded the information regarding this user to the HSI attaché office in Ottawa, Canada. HSI Ottawa conducted further research into IP address 76.184.73.204, learning that it was owned by Charter Communications and resolved to the Arlington, Texas area. Based on this information, the referral was forwarded to the HSI Dallas Child Exploitation Group for further investigation.

27. In September 2019, HSI Dallas received the information regarding user “bjm0907,” including the file that was flagged as suspected child pornography by the PhotoDNA software and subsequently reviewed by a Kik employee. The information provided for this image identifies the file as a “chat upload”, which indicates the file was distributed to at least one other Kik user. I reviewed the reported image, which is described as follows:

Hash Value	File Description
[redacted] B023B06.png	An image of a prepubescent female child lasciviously exposing her genitals, which is the focus of the camera. In addition, a white fluid like substance is observed on the prepubescent female’s genitals.

Based on my training and experience, this image meets the federal definition of child pornography, as defined in 18 U.S.C. § 2256.

28. Log-in data for the “bjm0907” Kik account indicates the individual controlling this account accessed the account using IP address 76.184.73.204 approximately 200 times between April 12, 2019 and May 13, 2019. These log-ins occurred on various dates, at different times of the day. Of note, Kik terminated this account on or about May 13, 2019 for distributing child pornography.

29. On October 4, 2019, HSI Dallas served a subpoena on Charter Communications for subscriber information relating to the customer(s) assigned IP address 76.184.73.204 on May 13, 2019. On October 11, 2019, Charter Communications complied with the subpoena and reported that this IP address was assigned to the following customer on the requested date:

Subscriber Name: Brett Monroe
Address: **5409 Windy Meadow Drive., Arlington, TX 76017**
IP Session: 03/14/2019 to 10/11/2019
Account creation date: 04/13/2017

30. During my investigation into this matter, I obtained a copy of the State of Texas driver’s license card for Brett Jarad Monroe. Monroe’s driver’s license indicates he was born [redacted] 1981, and lists a current address of **5409 Windy Meadow Drive, Arlington, Texas**. As disclosed in paragraph 25 of this affidavit, the individual who created Kik account “bjm0907” provided the same birthday of [redacted] 1981 during the account registration process. Furthermore, the Kik username initials “**bjm0907**” appears to match the driver’s license name of Brett Jarad Monroe.

During this investigation, I also researched the Consolidated Lead Evaluating Reporting (CLEAR) public records database for intelligence regarding residents associated with **5409 Windy Meadow Drive, Arlington, Texas**. CLEAR consolidated data indicates Brett Monroe is presently associated with the residence, as well as at least one other adult individual.

31. On November 26, 2019 through November 29, 2019, I conducted surveillance at **5409 Windy Meadow Drive, Arlington, Texas**. During this surveillance operation, I observed a vehicle with Texas license plate (last four-7186), registered to Jana and Brett Monroe with the same aforementioned address. Furthermore, I utilized a mobile electronic device to scan for wireless networks at or near this residence. While positioned directly in front of the residence, the device discovered multiple wireless networks. All of these networks were secured; therefore, there is probable cause to believe that **5409 Windy Meadow Drive, Arlington, Texas** is broadcasting a secured wireless network. Accordingly, an individual using the Internet services at this residence would likely need the encryption key or password to utilize its particular network.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

32. The facts contained in this affidavit establish probable cause to believe that an individual using the Internet services at **5409 Windy Meadow Drive, Arlington, Texas** has transported, distributed and possessed child pornography, or has attempted to commit said crimes, in violation of federal law.

Based on my training, experience, and numerous interviews of subjects who admitted to having a sexual interest in children, I am aware that the following characteristics are common to individuals involved in child pornography offenses:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity;

b. Such individuals may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts;

c. Such individuals often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines,

correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;

d. Such individuals often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like P2P file sharing. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection;

e. Such individuals often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer or surrounding area. These collections are often maintained for several years and are maintained at the individual's residence or place of employment, to afford immediate access to view the material;

f. Such individuals may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

33. The facts set forth in this affidavit demonstrate that an individual using the Internet services at **5409 Windy Meadow Drive, Arlington, Texas** meets the characteristics of a collector of child pornography because: 1) the individual

corresponded with other individuals online and used a profile to distribute child pornography; 2) this activity occurred on Kik, which is a mobile application that law enforcement knows to be a meeting place for individuals interested in sharing child pornography; and, 3) the individual accessed Kik approximately 200 times in a 30-day period, which based on my experience with Kik investigations, is indicative of an individual actively participating in sharing child pornography or exploiting children.

BIOMETRIC AUTHENTICATION ON DIGITAL DEVICES

34. Based on the facts set forth in this affidavit, and more specifically, the fact that Kik is an application only available for mobile devices, I believe that the premises to be searched will contain mobile electronic devices such as smartphones, tablets and e-readers, which will contain evidence subject to search and seizure under this warrant. Based on my training, experience, and publicly available information, I am aware that Apple, Motorola, and Samsung, as well as other companies, produce digital devices that can be unlocked via the use of a fingerprint or thumbprint in lieu of a numeric or alphanumeric passcode or password. Each company has a different name for this biometric authentication feature; for example, Apple's version is called "Touch ID."

35. If a user enables the Touch ID feature on an Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home button") at the bottom of the device.

Based on my training and experience, I am aware that users of Touch ID-capable devices often utilize this feature because it is a more convenient way to unlock the device, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activity and has a heightened concern about securing the contents of the device.

36. In some circumstances, a fingerprint cannot be used to unlock a Touch ID-enabled device, and a passcode or password must be used instead. These circumstances include: 1) when more than 48 hours have passed since the device has been unlocked; 2) when the device has been turned on or restarted; 3) when the device has received a remote lock command; or 4) after five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions for their biometric authentication features.

37. The passcode or password that may be needed to unlock the digital device(s) found during the search of **5409 Windy Meadow Drive, Arlington, Texas** is not known to law enforcement. Thus, it will likely be necessary to use the fingerprints or thumbprints of the user(s) of any fingerprint sensor-enabled device(s) found during the search, in order to unlock the device(s) for the purpose of searching for the evidence subject to seizure under this warrant.

38. Therefore, I request the authority to compel the use of the fingerprint(s) or thumbprint(s) of any person who is located at **5409 Windy Meadow Drive, Arlington, Texas** during the execution of the search, who is reasonably believed by law enforcement

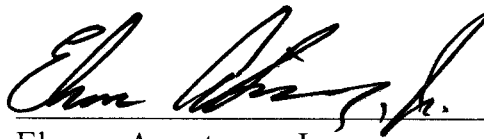
to be the user of a fingerprint sensor-enabled device located at this residence. The requested authorization is necessary because the Government may not otherwise be able to access the data contained on these devices for the purpose of searching for the evidence subject to seizure under this warrant.

CONCLUSION

39. Based on the information set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A are presently located at **5409 Windy Meadow Drive, Arlington, Texas**, and the digital media therein. Accordingly, I respectfully request that this Court authorize the search of this residence, including any vehicles located at or near the premises that fall under the dominion and control of the persons associated with said premises, so that agents may seize the items listed in Attachment B.

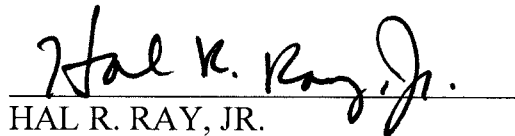
40. Rule 41 of the Federal Rules of Criminal Procedure authorizes the Government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them. I further request that the Court authorize the transfer of any computers, computer storage devices or smartphones to other Government authorized personnel or contractors, within or outside of this District, in the event that advanced expertise is needed to access the files subject to search and seizure under this warrant.

41. Because multiple people share the premises described in Attachment A as a residence, it is possible that there will be computers and storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, this application seeks permission to search, and if necessary to seize, those items as well. It may be impossible to determine on scene which computers or storage media contain the things described in this warrant.



Elmore Armstrong, Jr.
Special Agent
Homeland Security Investigations

Sworn to before me and subscribed in my presence this 9TH day of December 2019, at 2:38 p. m. in Fort Worth, Texas.



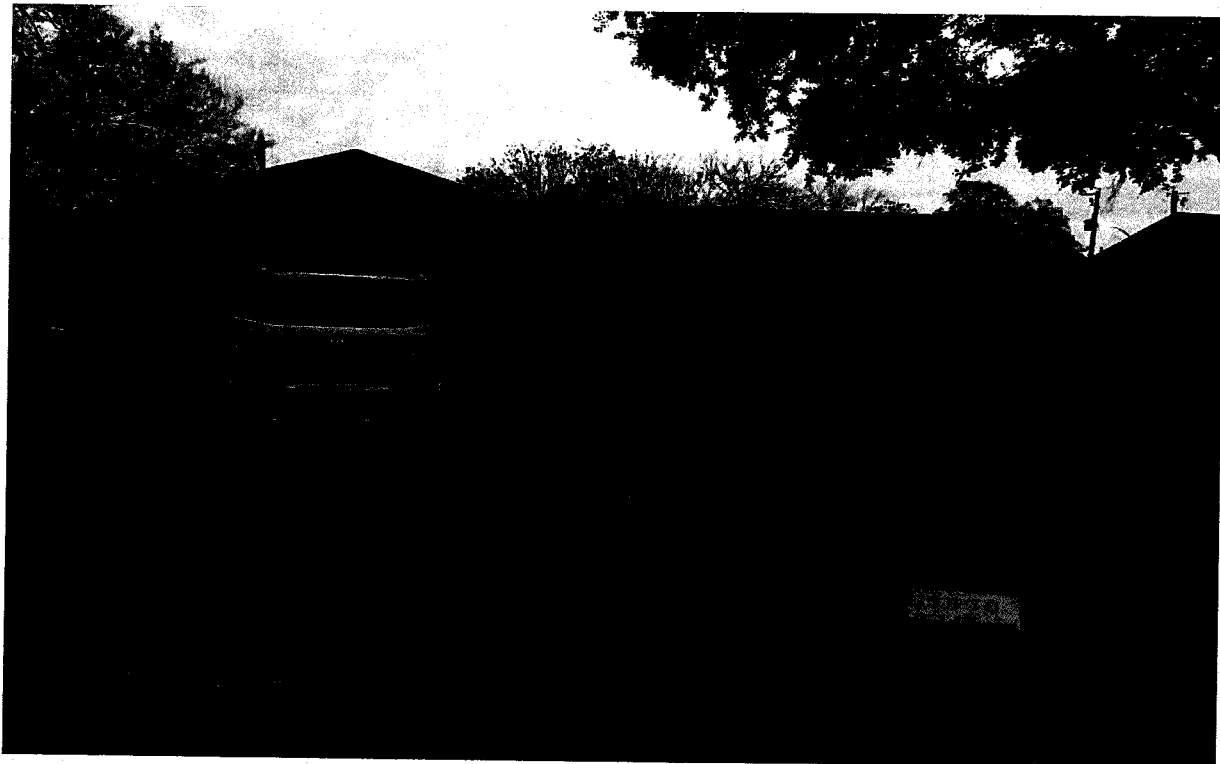
HAL R. RAY, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

5409 Windy Meadow Drive, Arlington, Texas 76107

The residence is described as a one-story, single-family dwelling constructed primarily of brick. The structure has brown and greyish blue trim, and the numbers "5409" are displayed on the right side of the driveway curb. The residence is located in Arlington, Tarrant County, Texas, within the Northern District of Texas. The search warrant includes any vehicles located at or on the premises, or within the curtilage of the premises, which fall under the dominion and control of any person(s) associated with, or present on, said premises. The search of these vehicles is to include all internal and external compartments or containers, which may reasonably store child pornographic materials. or their instrumentalities.



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Cell phones, to include iPhones, computers, tablets, computer hardware, computer software, computer related documentation, computer passwords and data security devices, cellular devices, video recording devices, video recording players, videotapes and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children or the coercion or enticement of children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Evidence identifying the individual(s) who used, owned, or controlled the computer(s) and cellular devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

3. For any computer, computer hard drive, cellular phone, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that may contain things otherwise called for by this warrant:

- a. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

- b. evidence of the lack of such malicious software;
- c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- e. evidence of the times the COMPUTER was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- h. contextual information necessary to understand the evidence described in this attachment.

4. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

5. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the

possession, receipt, or distribution of child pornography as defined in 18 U.S.C.

§ 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Any and all cameras, film, videotapes or other photographic equipment.

8. During the execution of this search warrant, law enforcement personnel are authorized to press the fingerprints and/or thumbprints of any person located at the residence during the execution of this warrant, to the fingerprint sensor of any device reasonably believed by law enforcement to be used by the person, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.